

Security: Built-in, Not Bolted On!

Open Source & Security

WATSH

Sept. 4, 2002



Shawn Geddis

Federal Senior Systems Engineer, Apple

geddis@apple.com

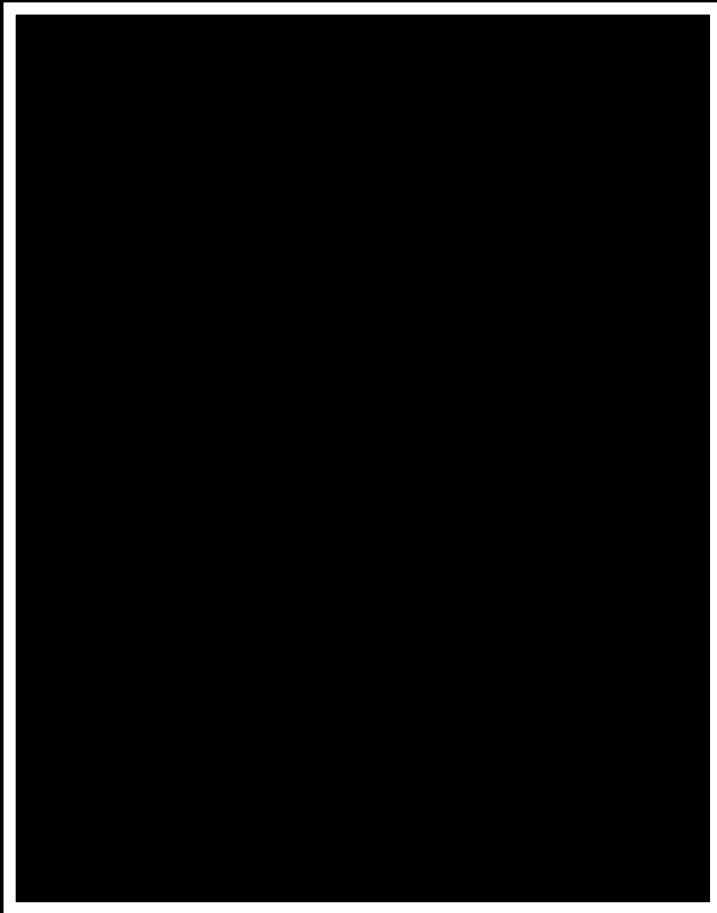


Shawn Geddis

Chairman, [STOS] Consortium

geddis@stosc.com

Security is not a luxury



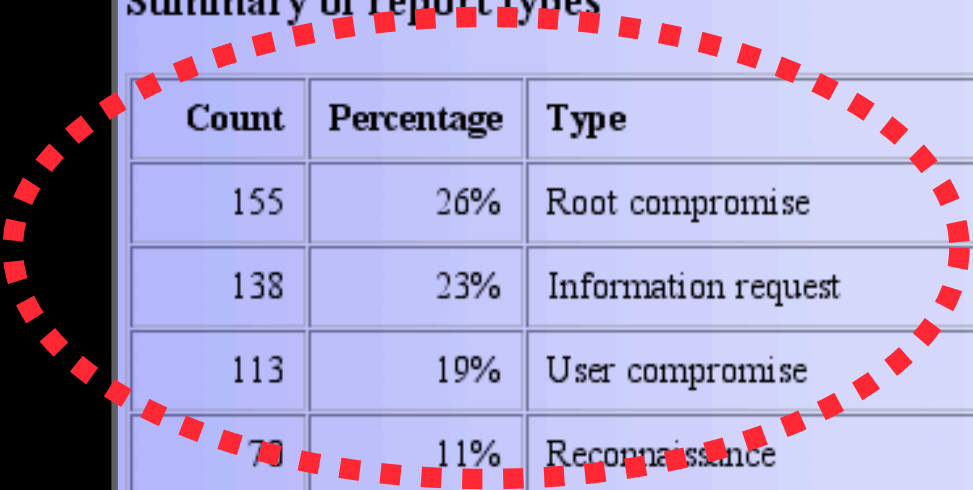
- New Types of Attackers
- New Types of Vulnerabilities
- Same Old Add-on Tools
- Same Old Defense

State of OS Security

FedCIRC Incident Activity Summary for 2000

A total of 586 reports involving 575,568 hosts reported to FedCIRC and the CERT[®]/CC were closed in 2000.

Summary of report types



Count	Percentage	Type
155	26%	Root compromise
138	23%	Information request
113	19%	User compromise
70	11%	Reconnaissance
36	6%	Virus
35	5%	Denial of service

Apple's Unique Position

Integration of hardware and software

- Hardware
- Firmware
- Operating system



Security in Hardware

Physical security

- Boot OS/Volume lockdown
Open Firmware Security – IEEE 1275
- Wireless Encryption and Authorization
128 and 40 bit WEP, RADIUS, Cisco LEAP
- Physical Case lockout
All desktop models: case lock slots
Kensington Cable Anchor ports on all



Open Firmware Security

IEEE 1275 security compliance

- Prevents use of Open Firmware hot keys:
 - “C” to boot from CD
 - “T” for FireWire target disk mode
 - “S” for single user mode
 - “N” to boot from a NetBoot server
- Boot device selector asks for password
- ⌘-option-P-R to reset parameter RAM
- ⌘-option-O-F Open Firmware commands require password
- Equivalent to setenv security-mode command
- Works on machines with updatable firmware



Mac OS X Architecture



User Interface

Frameworks

Graphics

UNIX-Based Foundation

Mac OS X & Open Source



Aqua

Frameworks

Graphics

UNIX-Based Foundation

Open Source

Community development, enhancing the foundations

Aqua

Frameworks

Graphics

UNIX-Based Foundation

- Full open source development model
- Over 100,000 people using live source code
- Enhanced Security and Trust thru peer review
- Rapid bug fixes

Darwin in Mac OS X

- Darwin = Mac OS X Core OS
- Can swap a Darwin kernel into Mac OS X

User Interface

Frameworks

Graphics

Darwin

Darwin Kernel

Combining compatibility and flexibility with innovation

- Compatibility: BSD 4.4
- Flexibility: Mach 3
- Innovation: Apple
 - Plug-and-Play drivers
 - Responsive multimedia
 - Instant sleep/wake
 - Seamless mobility

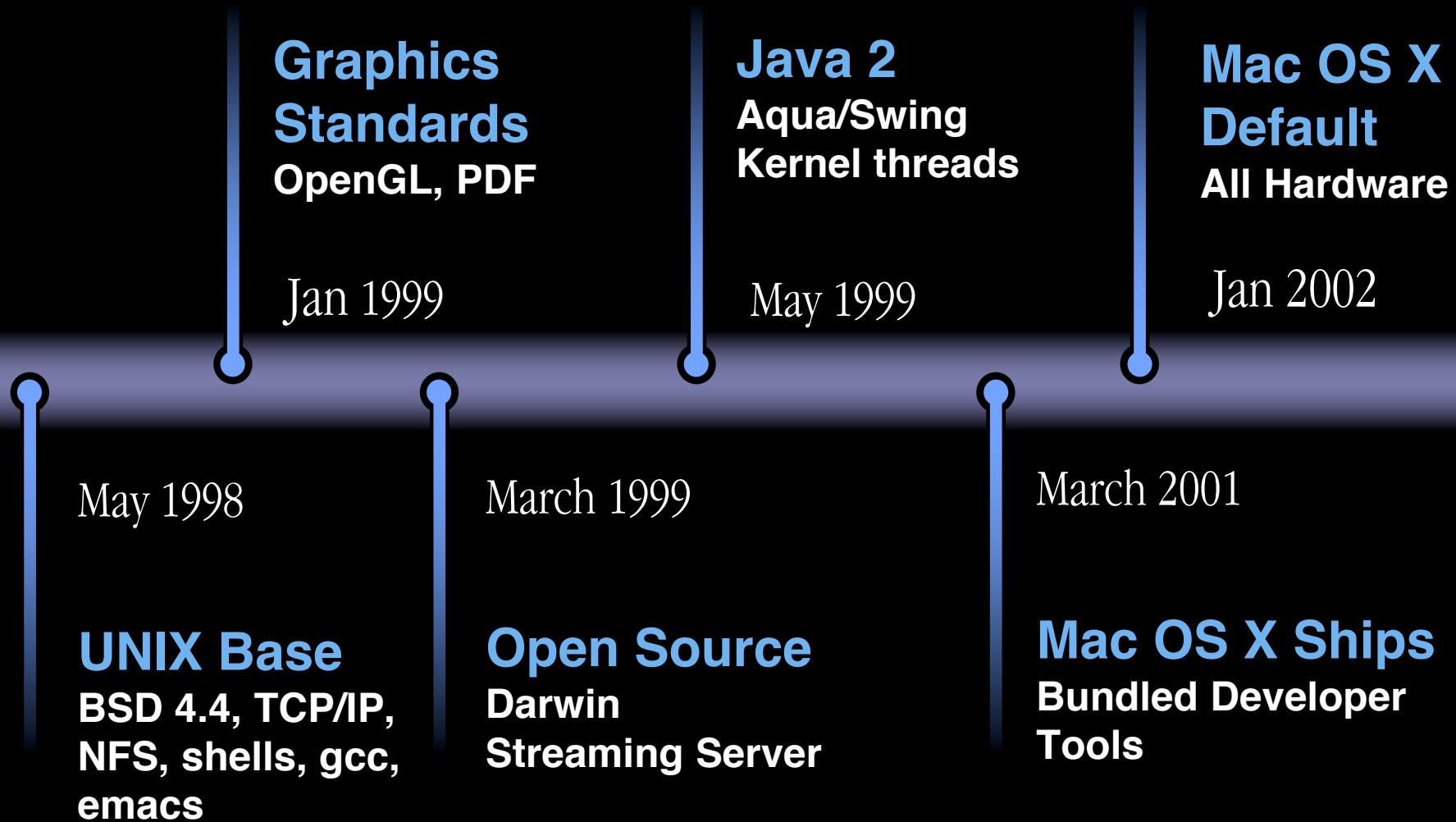
Kernel level Security

Security from the ground up

- Mac OS X more secure by default
 - All services off
 - No open ports by default
 - Root account disabled by default
 - Uses SSH instead of Telnet by default
 - File sharing (AFP, SMB, FTP) is off by default
- Protected memory
- File level permissions
- Built in firewall (ipfw)



Four Years in the Making



Community Respect

“Apple 'gets' Open Source. They know it's all about collaboration with their developer and user communities, as well as the broader Open Source community. They understand this positive feedback loop results in better software, and have figured out how to build a real business model around it. They are definitely setting the standard here.”



Brian Behlendorf

Apache Software Foundation

Open Source

Community development, enhancing the foundations

www.Apple.com/OpenSource

Open Source Projects Information



- CVS maintained outside of Apple
- Small number of “direct” outside committers
- Anyone can submit via website or email

Open Source

Community development, enhancing the foundations

www.OpenDarwin.org
Open Sandbox for all to play



- Maintained by the Internet Software Consortium, Inc. (ISC)
- Many, many “direct” outside committers
- Many more can signup / submit projects

Open Source

Community development, enhancing the foundations

www.STOSDarwin.org

Sandbox for security enhancements



- Maintained by the [STOS] Secure Trusted OS Consortium
- “SE-Darwin” - building from prior Trusted Mach kernel efforts
- Many more can submit / join projects

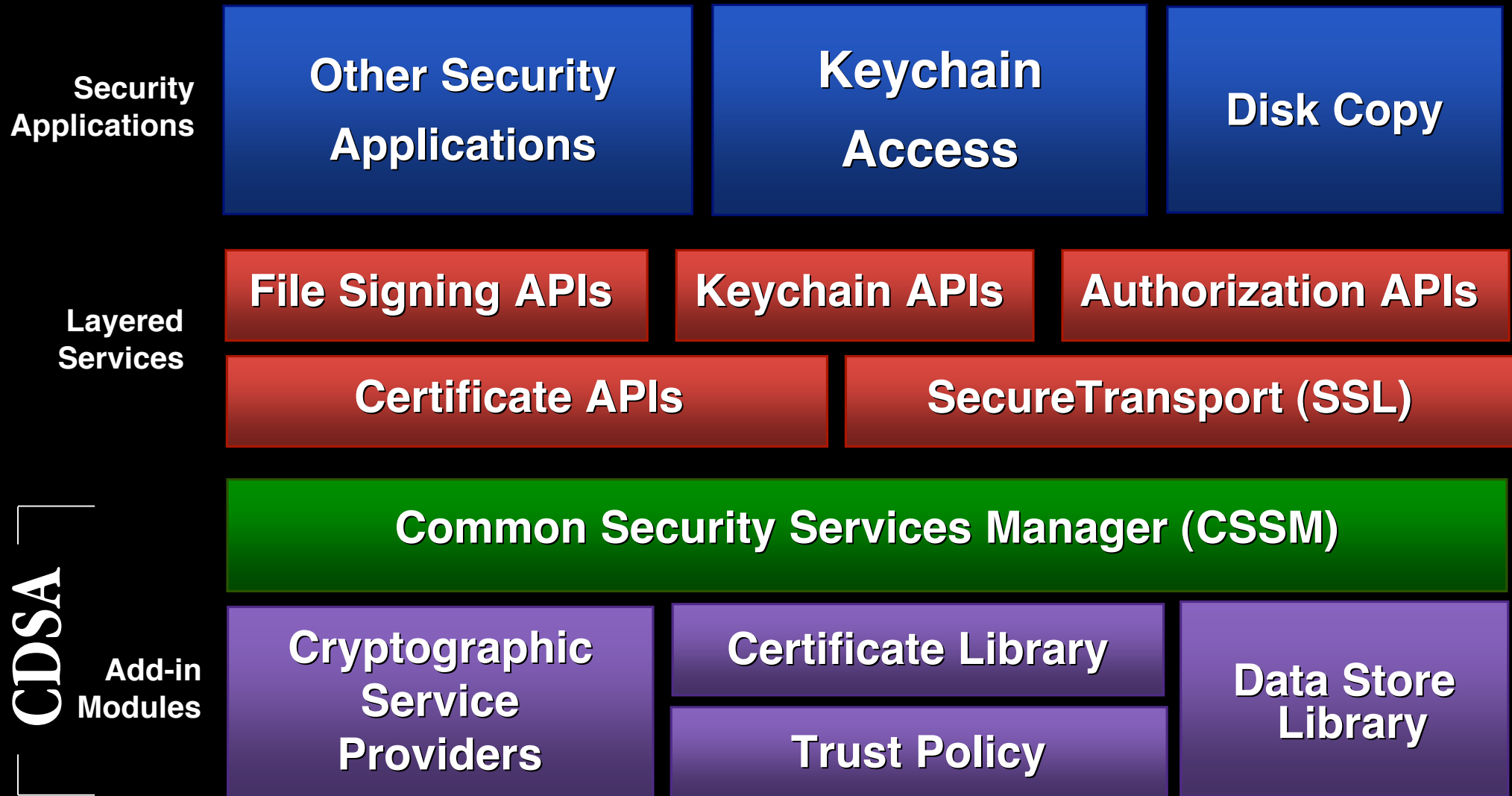
Common Data Security Architecture (CDSA)

- Provides plug-in architecture for different module types
- Apple provides standard modules;
 developers will add their own
- Fully standards-compliant implementation, based on
 The OpenGroup standard **C914**

www.OpenGroup.org

Common Data Security Architecture

Foundation for Cryptography and PKI



(CSP) Cryptographic Service Provider Modules

Provide-low level cryptographic operations

Encrypt/decrypt (RSA, DES)

Digest (MD5, SHA1)

Sign/verify (RSA, Diffie Hellman)

GenerateMac/VerifyMac (HMAC SHA1)

Wrap/unwrap of keys

Key generation/derivation (PKCS #5)

Random number generation



CSSM



CSP

(DL) Data Library Modules

CSSM

**Datastore
Library**

- Store information used by applications or other CDSA modules
- Provides abstraction from the underlying database
- Apple provides a multiservice CSP/DL module that can securely store keys
 - ✓ **Keychains** are files maintained by this CSP/DL
- Other DL modules could be made which look in an LDAP directory for certificates

(CL) Certificate Library Modules

- Parse certificates and Certificate Revocation Lists



CSSM



**Certificate
Library**

- Apple provides an X.509v3 capable CL
- Other CL modules might parse PGP or Attribute certificates

(TP) Trust Policy Modules



CSSM



Trust
Policy

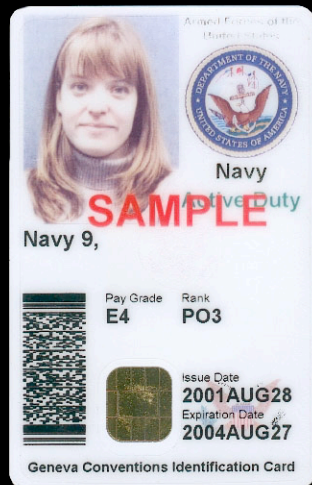
- Determine whether a particular group of certificates should be trusted
 - ✓ *Apple provides a configurable X.509 TP*
 - ✓ *A corporate TP could accept only particular certificate chains*
- Handle certificate issuance for one or more Certificate Authorities (CAs)
 - ✓ *A CA could write their own TP module to issue certificates to customers*

Common Access Card

- Contains 3 X.509v3 certificates:
 - ✓ Identity
 - ✓ Signing
 - ✓ Encryption
- DoD is driving adoption of Smart Cards
- JavaCard applet on card



OS X Smartcard Support



- Full PC/SC support
- Out of the box support for major USB smartcard readers
- Plugin architecture for readers and cards

Open Source

Community development for Smart Cards

www.LinuxNet.com

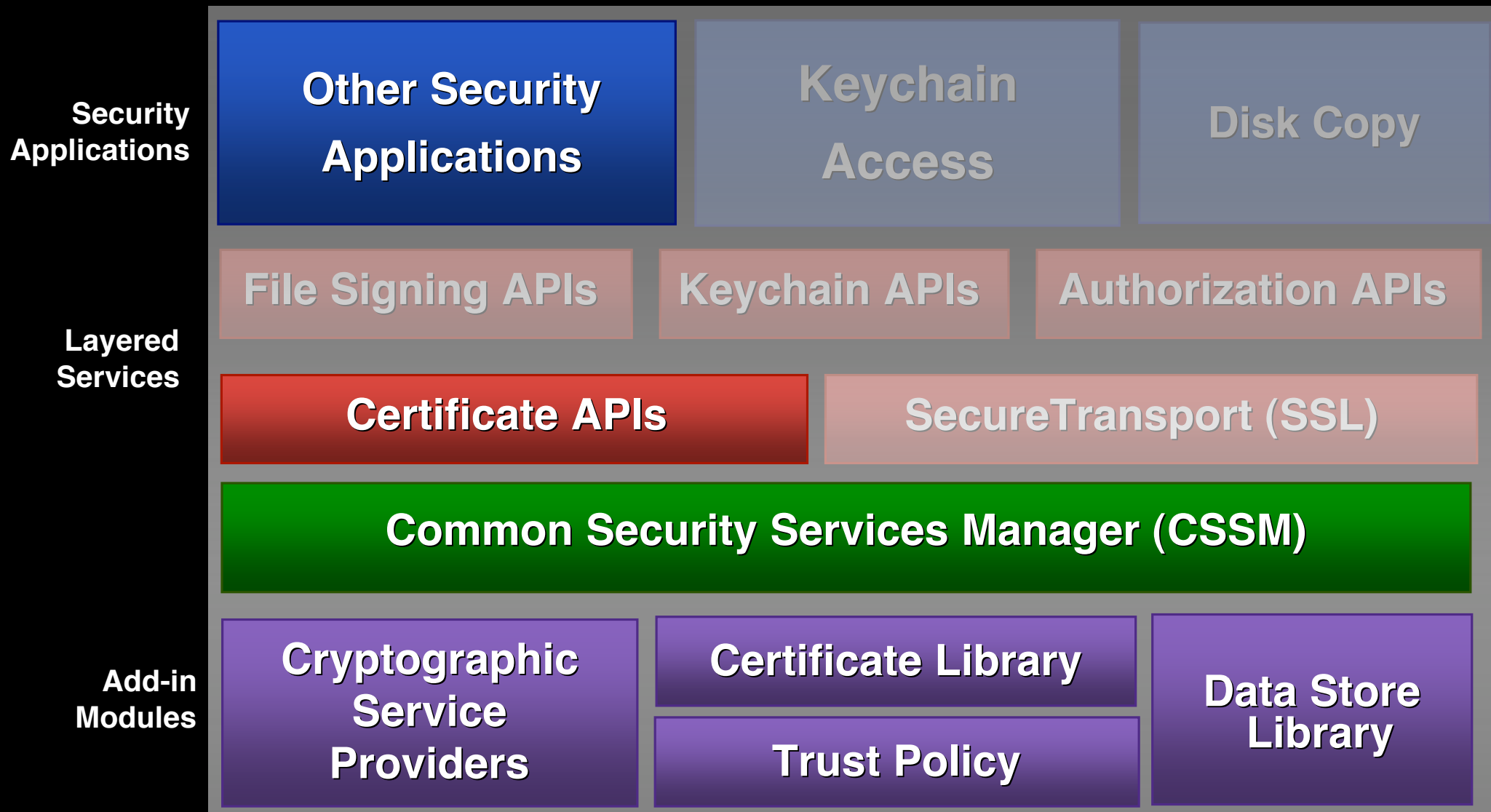
M.U.S.C.L.E. website

- M.U.S.C.L.E.
Movement for the Use of Smart Cards
in a Linux Environment
- Drivers for the major Smart Card Readers
Under multiple platforms
- David Corcoran

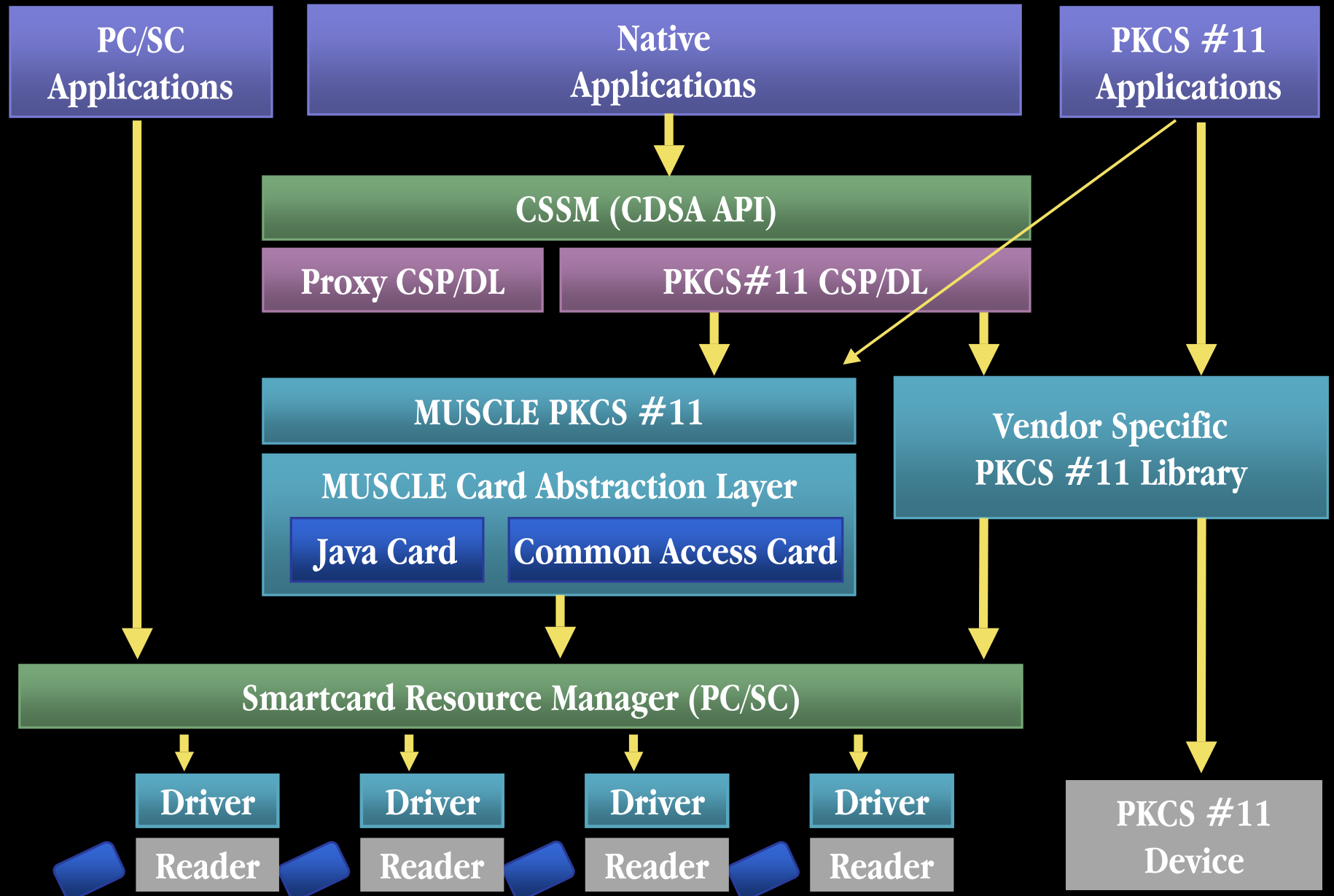
M.U.S.C.L.E.

Common Data Security Architecture

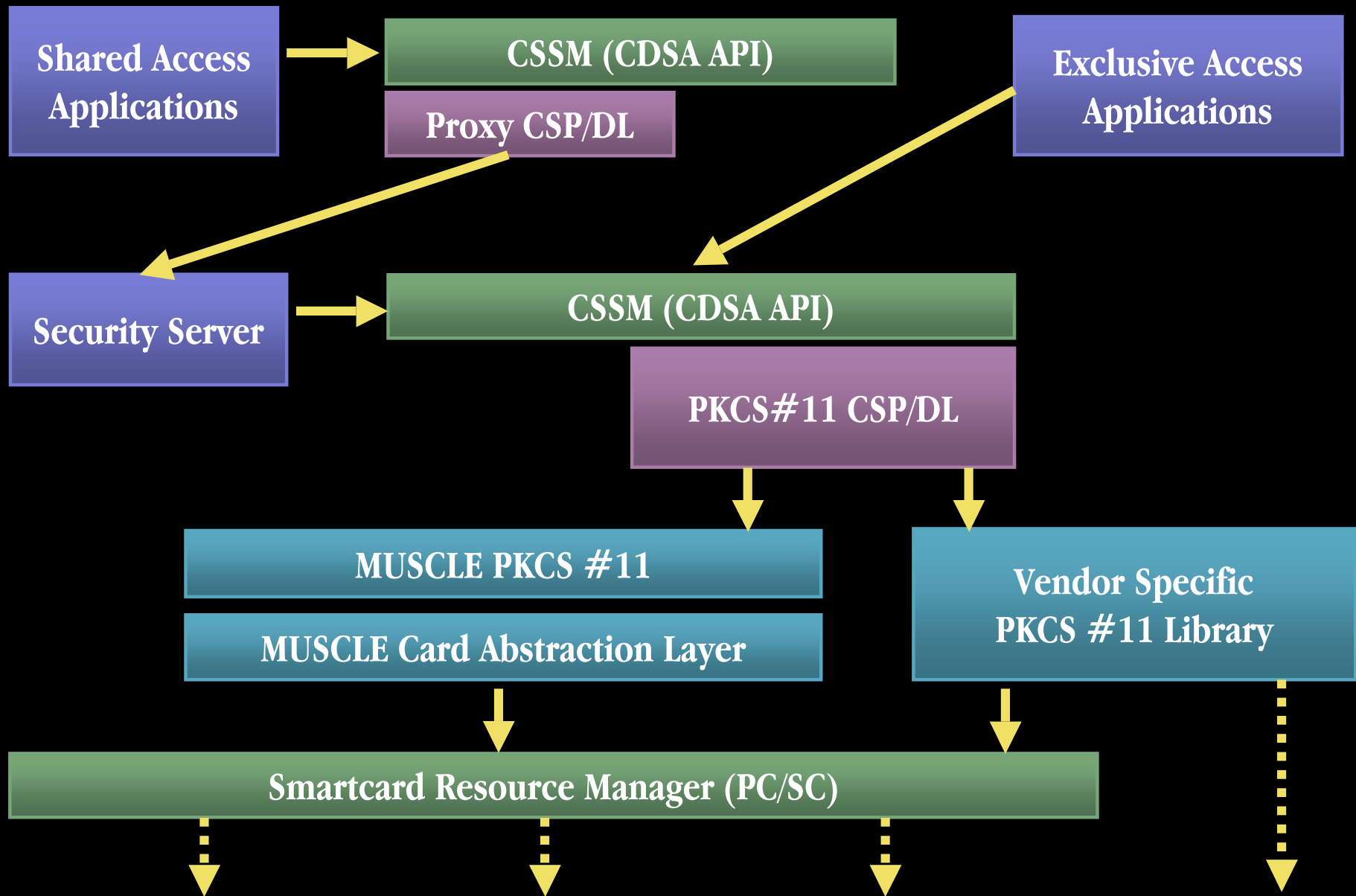
Foundation for Cryptography and PKI - SmartCards



Smartcard Architecture



Shared vs. Exclusive Access



Protecting your data

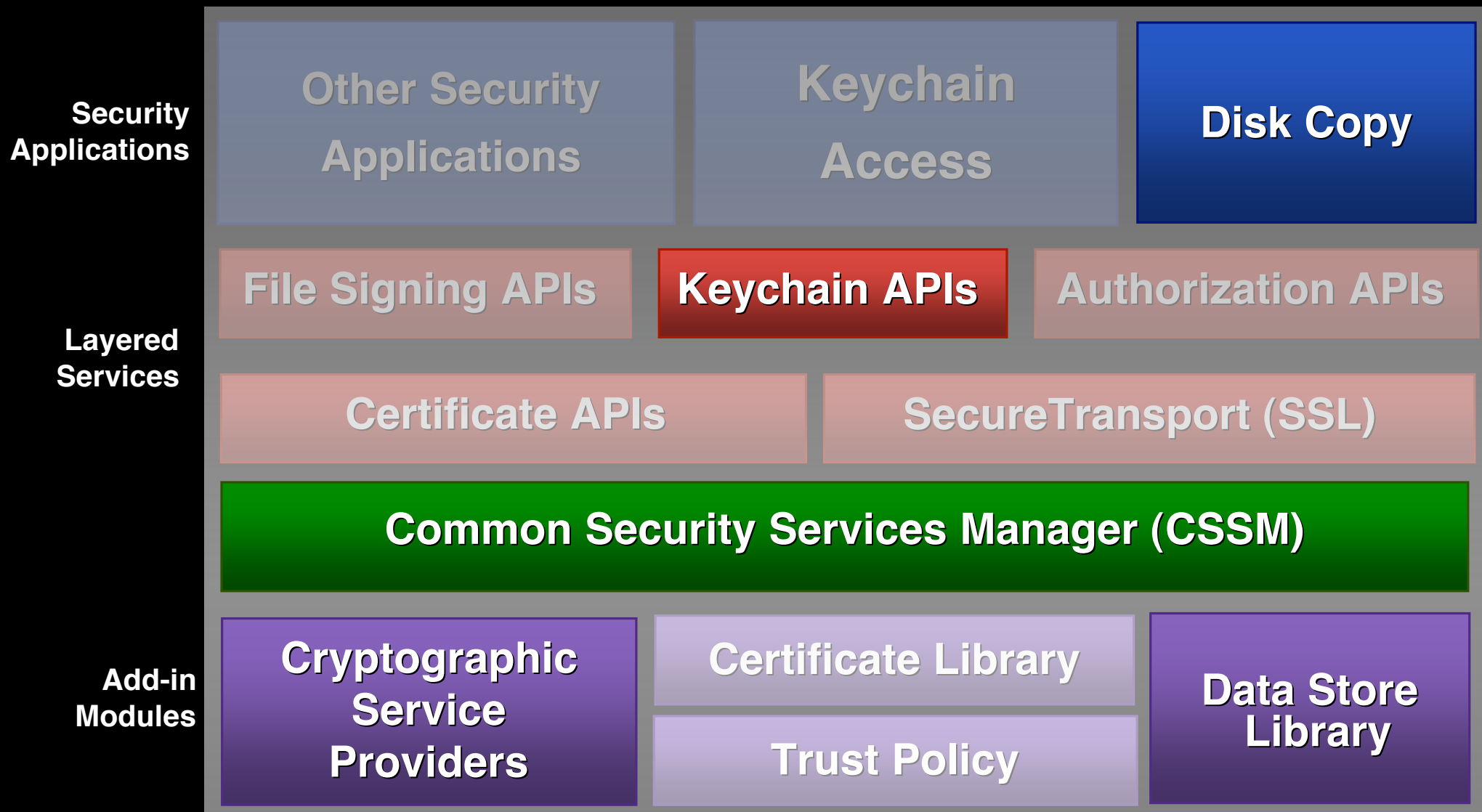
High grade AES-128 encryption



- Encrypted Disk Copy images
- Appear like any other volume
- High performance
- Built on top of CDSA — easy to change algorithm or use hardware cryptography

Common Data Security Architecture

Encrypted Disk Copy Images



Encrypted Disk Copy Images

- Choose “New Blank Image”
- Type file name in “Save As”
- Select a location for the file
- Type in name for the volume in “Volume Name”
- Select a size for image file
- Choose format for volume
- Select “AES-128” under the “Encryption” popup menu
- Click the “Create” button



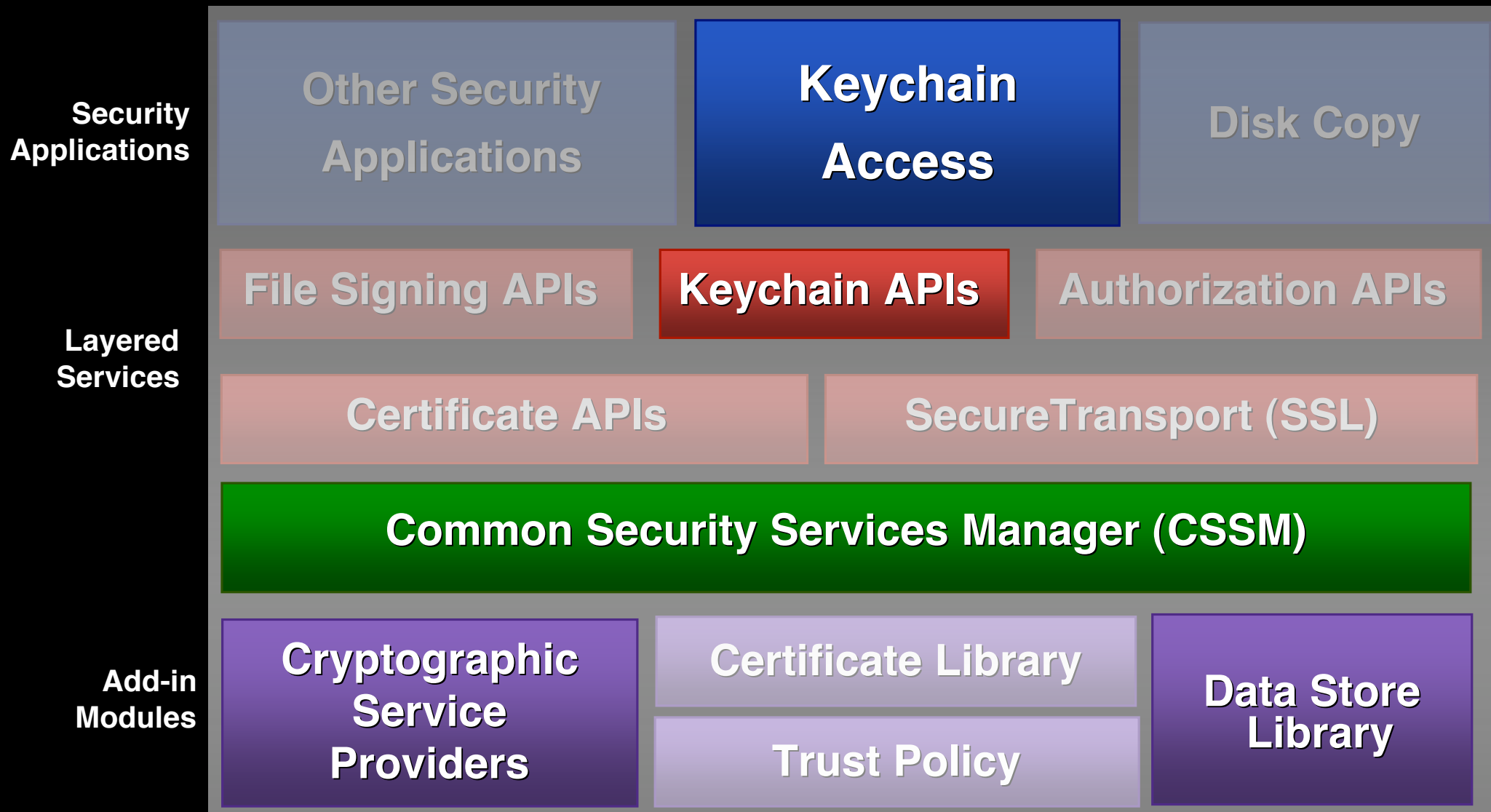
Keychain

- Every user on Mac OS X has a Keychain
- Unlocked with login password
- Multiple keychains are supported
- More secure than ad-hoc solutions
- Long keychain passwords supported
- If you need to save a password somewhere, use the Keychain!



Common Data Security Architecture

Secure storage of Credentials

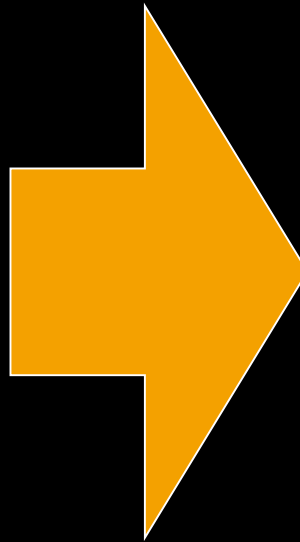


NIST Security APIs

High-level API for PKI

--NIST--

- nist_signBuffer
- nist_signFile
- nist_verifyBuffer
- nist_verifyFile
- nist_encryptBuffer



--CDSA--

- CSSM_Sign_Data
- CSSM_Digest_Data
- CSSM_Verify_Data
- Digest then verify
- CSSM_Encrypt_Data

<http://csrc.nist.gov/pki/pkiapi/welcome.htm>

Apple's Security Efforts

What is Apple doing to ensure security?

- Apple Product Security Team
Work closely with CERT, FIRST, FreeBSD and others
- Product Security Web Page
<http://www.apple.com/support/security>
- Apple Security Updates
Urgent security updates via Software Updates
http://www.apple.com/support/security/security_updates.html
- Darwin and the open source community

Apple's Security Efforts

Apple and Federal Government ensuring security

- [STOS] Secure Trusted OS Consortium
 - Federal, Academia and Industry
- *CHATS* - DARPA/ATO - Doug Maughan
 - Security enhancements to Open Source Operating Systems
BSD (FreeBSD, OpenBSD, NetBSD, Darwin), Linux, ...
- Trusted OS Collaboration - NSA
 - “SE-Darwin” - DTOS Comparison (Trusted Mach)
- SmartCard / CAC - NMCI - DON CIO
 - Built-in support for (3) DoD Certificates / Java 2.1 Applet
 - Collaboration on Smart Card Open Source efforts

Apple's Security Efforts

Apple, Federal and others ensuring security

- **NIST - *PKI***
 - **Federal PKI - Technical Working Group (FPKI-TWG)**
 - **High-level PKI API**
 - **GAO-FDIC-NIST PKI Sanctions**
- **MIT - *Kerberos***
 - **Combined v4 & v5 with Single Sign-on**
 - **Shipped in OS X 10.1 (Sept. 2001)**

Common Criteria

Level playing field for security evaluations

- Completed the *Initial Assessment* of Mac OS X
 - Jan 14 - 17, 2002
- “In Evaluation” as of June 27, 2002
 - NIAP Acceptance of Security Target and Plan
 - CAPP / EAL3
 - Controlled Access Protection Profile
 - Evaluation Assurance Level 3
- Critical Dates for Federal Government (*NSTISSP#11*)
 - Jan 1, 2001 - “Preferred” acquisition to certified products
 - July 1, 2002 - Acquisition “Limited” to certified products*

* Federal Government appears to be struggling to enforce this within agencies

[STOS] Consortium



Secure
Trusted
Operating
System

[STOS] Consortium

A cooperative and collaborative arrangement to:

*Engage in the evolution of high volume
secure, trusted operating systems through
open and collaborative research,
development and training based on
Darwin / BSD Open Source Projects.*

Role in Mac OS X Evolution

“Help us [Apple] build a Secure, Trusted OS and we’ll ship it as a Commercial OS.”

*Avadis Tevanian, Jr., Ph.D.
Senior Vice President
Apple Computer*

Open Collaboration



~ **440 Members**

~ **90 Organizations**

Government

Academia

Industry

When and Where

Launch
Reston, VA

Aug 2000

Nov 2000

Direction
Reston, VA

**Power &
Progress**
Cupertino, CA

Aug 2001

May 2001

**State of the
Union**
San Jose, CA

Progress
San Jose, CA

May 2002

Feb 2002

**Building on
Strength**
Chantilly, VA

**Mac OS X &
BSD Security
Symposium**
Monterey, CA

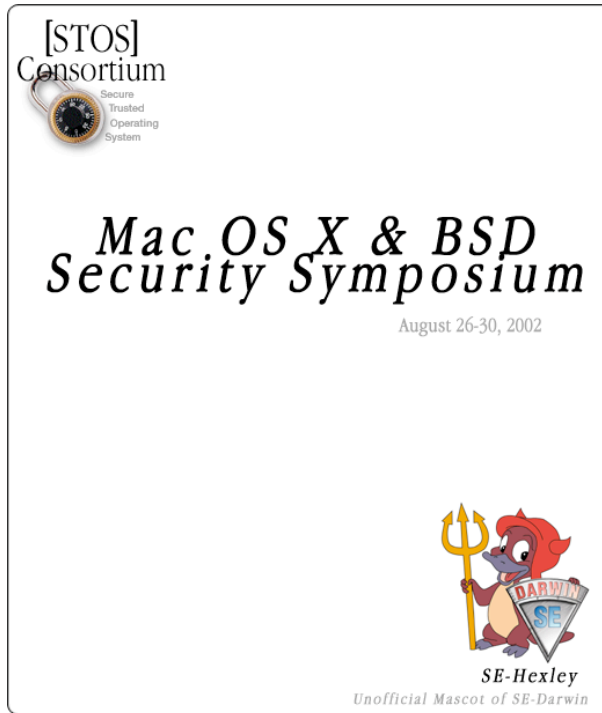
Aug 26 - 30 2002

Feb 2003

TBD

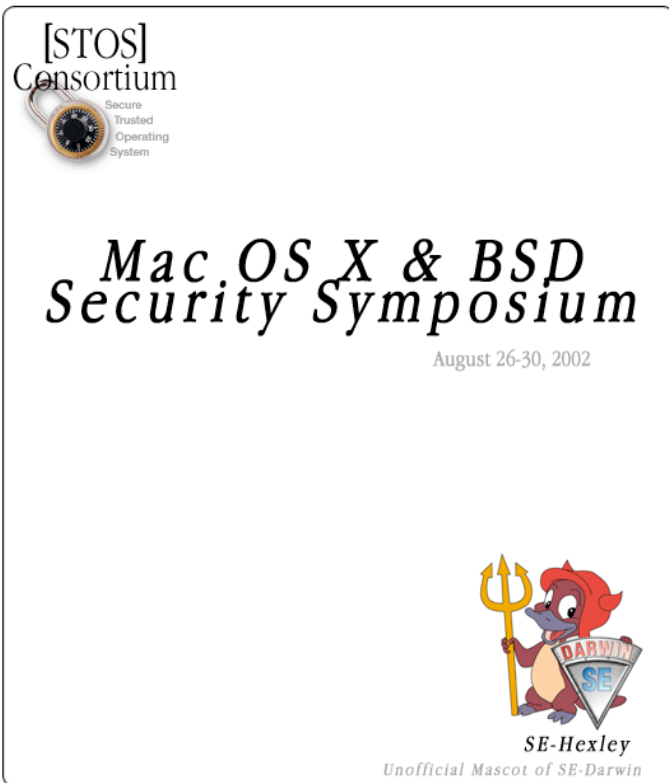
Washington, DC

© 2002 Apple Computer



Mac OS X & BSD Security Symposium

August 26-30, 2002
Monterey, CA

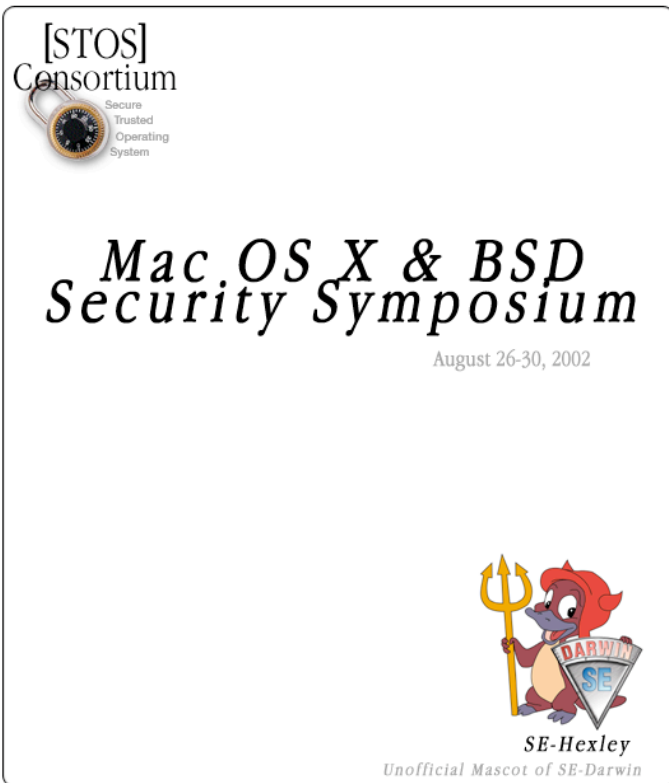


Keith Schwalm

Director of Infrastructure Protection

President's Critical infrastructure Protection Board

Wednesday Keynote



Paul Pittelli

**Chief,
Information Assurance Research Group**

National Security Agency

Thursday Keynote

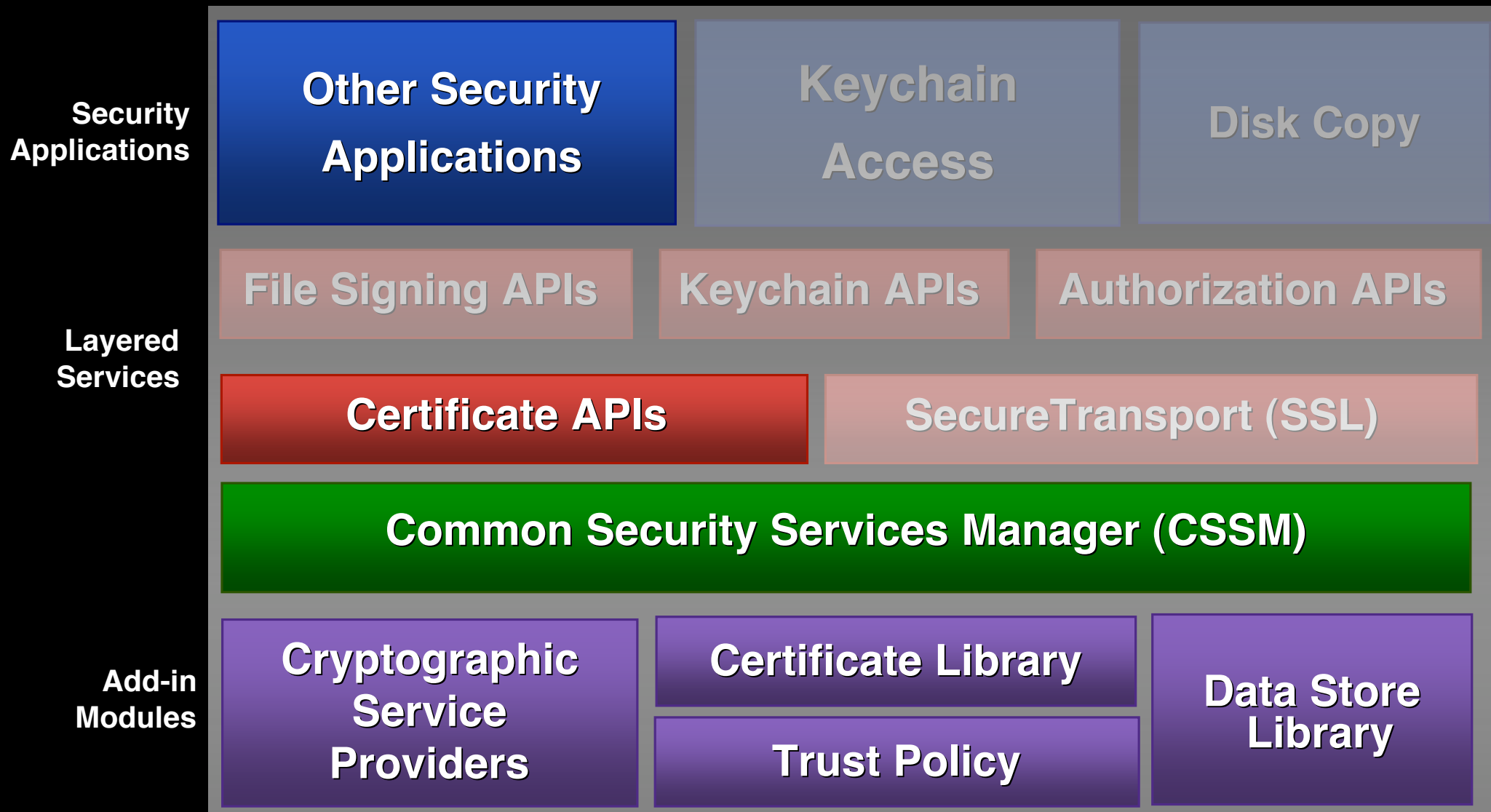
Proposed Project

Open Source PKI / SmartCard

- Leverage CDSA as powerful and existing open source Crypto & PKI architecture
- CDSA is available for:
 Darwin, Linux, AIX, FreeBSD, Windows, ...
- Bring the various implementations into sync

Common Data Security Architecture

Foundation for Cryptography and PKI - SmartCards



Cyberdiversity

Multiple operating systems for survivability

- Can you afford to be without e-mail for a day?
- Monoculture can be catastrophic
 - “The Nimda worm, which alone did \$2 billion in damage, hit many banking institutions that thought they were doing a good job on cybersecurity”, [Richard Clarke] said.
- Heterogeneous environments are resilient
 - More support overhead, but predictable
 - Cross-platform viruses extremely rare
- Web services are platform agnostic

Summary

Apple is serious about security

- Mac OS X leverages Unix security
- More secure out of the box
- Support for security built in at all levels

Resources

Security

Specifications and SDKs for developers

<http://developer.apple.com/macos/security.html>

CDSA 2.0

Specifications

<http://www.opengroup.org>

PC/SC

Specifications

<http://www.pcscworkgroup.com>

Open Source

Apple's open source repository

<http://opensource.apple.com/>

Product Security

Apple's security information and reporting page

<http://support.apple.com/security>

Who to Contact

Apple Federal Systems

Shawn Geddis

Federal Senior Systems Engineer

geddis@apple.com

Worldwide Developer Relations

Craig Keithley

Security & Cryptography Technology Manager

keithley@apple.com

Software Engineering

John Hurley, Ph.D.

Security Policy Architect

jhurley@apple.com

Q & A